CreateProcess-02

Parent process has explicit trust from child

Sean Barnum, Cigital, Inc. [vita¹]

Copyright © 2007 Cigital, Inc.

2007-03-20

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 4800 bytes

Attack Category	Privilege Ex	Privilege Exploitation			
Vulnerability Category		Process management			
Software Context	Threads and	Threads and Processes			
Location					
Description	In calling CreateF handle and proces These handles are completely rewrit WriteProcessMenthat the child process	Parent process has explicit trust from child. In calling CreateProcess(), you receive a thread handle and process handle to the child process. These handles are sufficient to allow the parent to completely rewrite the child using functions such as WriteProcessMemory. An interesting result of this is that the child process must trust your parent process. A parent always has the ability to rewrite the child.			
APIs	FunctionName		Comme	Comments	
	CreateProcess				
	CreateProcessA	CreateProcessA A		ANSII implementation	
	CreateProcessW	teProcessW Ur		Unicode implementation	
	CreateProcessAs	CreateProcessAsUser			
	CreateProcessWi	CreateProcessWithLogonW			
Method of Attack		Just a warning: you must trust your parent. Parent can overwrite process image.			
Exception Criteria					
Solutions	Solution Applicability			Solution Efficacy	
	Child process handles sensitive data or operations that parent should not have access to.	Child process should not do anything that it would be catastrophic for the parent to have access to.		Effective, but may conceivably mean some things can't be done.	

 $^{1. \}quad http://buildsecurityin.us-cert.gov/bsi/about_us/authors/35-BSI.html~(Barnum, Sean)\\$

CreateProcess-02

Signature Details	BOOL CreateProcess(
	LPCTSTR lpApplicationName,	
	LPTSTR lpCommandLine,	
	LPSECURITY_ATTRIBUTES lpProcessAttributes,	
	LPSECURITY_ATTRIBUTES lpThreadAttributes,	
	BOOL bInheritHandles,	
	DWORD dwCreationFlags,	
	LPVOID lpEnvironment,	
	LPCTSTR lpCurrentDirectory,	
	LPSTARTUPINFO lpStartupInfo,	
	LPPROCESS_INFORMATION	
	lpProcessInformation	
); POOL Great Person A. Henri	
	BOOL CreateProcessAsUser(
	HANDLE hToken,	
	LPCTSTR lpApplicationName,	
	LPTSTR lpCommandLine,	
	LPSECURITY_ATTRIBUTES lpProcessAttributes LPSECURITY_ATTRIBUTES lpThreadAttributes,	
	BOOL bInheritHandles,	
	DWORD dwCreationFlags,	
	LPVOID lpEnvironment,	
	LPCTSTR lpCurrentDirectory,	
	LPSTARTUPINFO lpStartupInfo,	
	LPPROCESS_INFORMATION	
	lpProcessInformation	
);	
	BOOL CreateProcessWithLogonW(
	LPCWSTR lpUsername,	
	LPCWSTR lpDomain,	
	LPCWSTR lpPassword,	
	DWORD dwLogonFlags,	
	LPCWSTR lpApplicationName,	
	LPWSTR lpCommandLine,	
	DWORD dwCreationFlags,	
	LPVOID lpEnvironment,	
	LPCWSTR lpCurrentDirectory,	
	LPSTARTUPINFOW lpStartupInfo,	
	LPPROCESS_INFORMATION lpProcessInfo	
);	
Examples of Incorrect Code	/* In child process */	
	doSomethingParentShouldNotHaveAccessT	
Examples of Corrected Code	doSomethingParentShouldNotHaveAccessT /* In child process */	
Examples of Corrected Code		
Examples of Corrected Code	/* In child process */	
Examples of Corrected Code	/* In child process */ /* Should not include	
Examples of Corrected Code	/* In child process */ /* Should not include functionality if parent having	
Examples of Corrected Code Source Reference	/* In child process */ /* Should not include functionality if parent having access would be a serious problem.	
	/* In child process */ /* Should not include functionality if parent having access would be a serious problem. */	

CreateProcess-02

2

Recommended Resource		
Discriminant Set	Operating System	• Windows
	Languages	• C
		• C++

Cigital, Inc. Copyright

Copyright © Cigital, Inc. 2005-2007. Cigital retains copyrights to this material.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and "No Warranty" statements are included with all reproductions and derivative works.

For information regarding external or commercial use of copyrighted materials owned by Cigital, including information about "Fair Use," contact Cigital at copyright@cigital.com¹.

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

CreateProcess-02 3

^{1.} mailto:copyright@cigital.com